

# **Drive Crypt Plus Pack (DCPP) v3.XX**

## **Kurzanleitung**

Deutsche Ausgabe von Marvin Heimbrodt  
(marvinheimbrodt@arcor.de)

## **Drive Crypt Plus Pack in 10 Schritten benutzen**

**Sichere Festplattenverschlüsselung für Windows NT4, 2000, XP u. Vista**

**<http://www.securstar.com> [info@securstar.com](mailto:info@securstar.com)**

## Inhaltsverzeichnis

Inhaltsverzeichnis	2
Haftungsausschluss	3
Über Drive Crypt Plus Pack	4
Hauptfunktionen von Drive Crypt	6
1. DCPD installieren und löschen	8
2. DCPD benutzen	9
3. Anmeldung	13
4. Schlüssel	14
5. Laufwerke	16
6. Bootauth	17
7. Anmelden in DCPD	21
8. Verschlüssen eines Laufwerks	22
9. Erstellen eines Notfall- Reparatur Mediums	24
10. Notfall- Reparatur Medium einsetzen	27
11. Erstellen eines versteckten Betriebssystems	30

**Achtung:** Dies ist nur eine Kurzanleitung, die die Schritte zum Verschlüsseln zeigt. Bitte benutzen Sie die programmeigene Hilfe um detaillierte Informationen zu speziellen Funktionen zu bekommen. Diese Funktionen könnten Folgende sein:

- Verstecktes Betriebssystem erstellen
- Ändern des Passworts
- Benutzen eines USB- Token
- Benutzen der „Lockout Console“
- Roter Bildschirmmodes zum schützen vor Passwortklau

## Haftungsausschluss:

"Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen."

--Artikel 12 der Allgemeinen Erklärung der Menschenrechte --

Dieses Programm verwendet Methoden der Datenträgerverschlüsselung, um unberechtigten Zugriff auf gespeicherte Daten zu verhindern. Dies könnte als „Verschlüsselung“ interpretiert werden, und daher könnte die Verwendung dieses Programms in manchen Ländern eingeschränkt oder verboten sein.

Das Programm ist nicht für die Speicherung illegaler Daten vorgesehen, und eine solche Verwendung ist nicht die Zielsetzung der Programmierer oder der SecurStar GmbH bei der Bereitstellung dieses Dienstprogramms.

Die Autoren des Programms und die SecurStar GmbH können nicht verantwortlich gemacht werden für jeglichen Verlust von Daten aufgrund jeglicher Inkompatibilität des Programms beim Einsatz auf einer je spezifischen Hardware- und/oder Software-Konfiguration.

Mit der Verwendung des Programms erkennt die Person, die es installiert, ihre **EIGENE** Verantwortung an, ihre wichtigen Daten zu sichern, und ist hiermit ausdrücklich dazu aufgefordert, dies vor der Installation dieser Software zu tun.

Es ist eine Bedingung für die Anwendung, dass Datenverlust aufgrund eines jeglichen Programmier- oder Funktionsfehlers oder einer Betriebsstörung dieses Programms nicht in der Verantwortung der SecurStar GmbH liegt. **Im Zweifel sichern Sie Ihre Daten vor der Installation dieser Software** und vergewissern Sie sich der ordnungsgemäßen Funktion auf einem System, das keine unersetzlichen Daten enthält.

Die SecurStar GmbH trägt keine Verantwortung im Falle eines Verlustes des Passwortes, das für den Zugang zu verschlüsselten Daten benötigt wird, und

kann auch keinerlei Hilfe leisten.

## **Über Drive Crypt Plus Pack**

DriveCrypt Plus Pack (DCPP) bietet echte "on the fly" 256-Bit-Festplatten-verschlüsselung in Echtzeit. Durch die Gewährleistung fortschrittlicher FDE (Full disk encryption) im Gegensatz zur VDE (Virtual disk encryption) oder "Container"-Verschlüsselung, ist DCPP ein wichtiger Entwicklungsschritt auf dem Gebiet des transparenten Datenschutzes.

DCPP erlaubt Ihnen, Ihre Platte(n) (inklusive Wechselmedien) mit dem leistungsstarken und erprobten Verschlüsselungs-Algorithmus AES-256 auf Sektor-Ebene zu schützen. Dadurch wird sichergestellt, dass nur autorisierte Nutzer Zugriff erlangen.

Der von DCPP verwendete Verschlüsselungsalgorithmus ist zuverlässig und erprobt. Er wurde vom National Institute of Standards and Technology (NIST) ausgewählt und als kryptographischer Standard für viele kommende Jahre bezeichnet. AES-256 ist ein symmetrischer Verschlüsselungsalgorithmus nach FIPS-Standard, der von U.S. Regierungsorganisationen (und anderen) eingesetzt werden darf, um sensible Informationen zu schützen.

DCPP arbeitet automatisch und völlig transparent für den Nutzer. Dies verringert nicht nur die Anforderungen an die Anwender und damit den Schulungsbedarf, sondern schafft auch die Grundlage für durchsetzbare Sicherheit. Die sorgfältige Integration von Boot-Sicherung und automatischer Verschlüsselung bietet einen hohen Grad an Sicherheit bei minimalen Auswirkungen für die Benutzer.

Die Boot-Sicherung verhindert die Umgehung des Betriebssystems (z.B. über eine Startdiskette) oder das Aufspielen schädlicher Programme, während die Sektor-für-Sektor-Verschlüsselung es unmöglich macht, einzelne Dateien für Brute-force-Attacken zu kopieren.

DCPP schützt das Betriebssystem und wichtige Dateien (die oft Hinweise auf Passwörter für Windows enthalten). DCPP ist das schnellste und vielseitigste System zur Echtzeitverschlüsselung auf dem Markt. Besondere Mühe wurde darauf verwendet, alle kryptographischen Bestandteile so unsichtbar und transparent wie möglich zu gestalten.

DCPP erlaubt das Verstecken eines ganzen Betriebssystems im freien Platz eines anderen Betriebssystems. Falls Sie gezwungen werden, ein Passwort zu nennen, können Sie den Angreifer in die Irre leiten, indem Sie ihm ein "vorbereitetes" harmloses Betriebssystem zeigen, anstelle der wirklich vertraulichen Daten.

## Hauptfunktionen von Drive Crypt

- Boot-Sicherung
- Pre-Boot-Authentifizierung: Anmeldung vor dem Start des Betriebssystems
- Unterstützung für das Booten mehrerer Betriebssysteme
- Unsichtbares Betriebssystem (Möglichkeit, das gesamte Betriebssystem zu verstecken)
- Völlige oder teilweise Festplattenverschlüsselung
- Schutz auf Sektor-Ebene
- Vollständiger "Power-off"-Schutz, d.h. unbefugte Nutzer werden am Starten des PCs gehindert
- AES-256-bit Verschlüsselung
- Keine Größenbeschränkung für verschlüsselte Platten
- Bewältigt eine unbegrenzte Zahl verschlüsselter Platten gleichzeitig.
- Erlaubt Steganographie, um Daten in Bildern zu verstecken.
- Schutz vor Trojanern und Tastatur-Sniffen verhindert das Ausspionieren von Passwörtern (roter Bildschirmmodus).
- Mechanismen gegen Wörterbuch- und Brute-force-Attacken (seine Architektur macht DCCP zum am schwierigsten anzugreifenden System am Markt)
- Verschlüsselt so gut wie alle Medien (Festplatten, Disketten, ZIP, JAZ, etc...)
- Spezifische Rechte für Administratoren und User
- Authentifizierung über USB-Token auf der Pre-Boot-Ebene möglich (Rainbow iKey 10xx und Aladdin R2/Pro)
- Möglichkeit, die Integrität der Verschlüsselungsmethode zu überprüfen
- Recovery-Disk für Notfälle
- Einfache Installation und Bedienung

- Völlige Transparenz für den Anwender

## **Über diese Anleitung**

Diese Dokumentation beinhaltet eine Schritt für Schritt Anleitung um Drive Crypt Plus Pack(DCPP). Sie zeigt nur die Basisfunktionen um eine Festplatte zu verschlüsseln. Wenn Sie mehr über die Funktionen von Drive Crypt Plus Pack erfahren wollen schauen Sie bitte in die programmeigene Hilfe.

## 1. DCPD installieren und löschen

### 1.1.1 Systemvoraussetzungen

Drive Crypt Plus Pack stellt nur sehr niedrige Anforderungen an Ihr System

- Einen Computer mit Windows NT, 2000, XP oder Vista (Win. 95,98 u. ME werden **nicht** unterstützt!).
- Ca. 10MB freien Speicherplatz für die DCPD Installation.
- Eine VESA- kompatible SVGA Grafikkarte, die mindestens 800 x 600 mit 256 Farben.
- Ein Diskettenlaufwerk(Floppy) oder ein CD- RW Laufwerk(CD- Brenner) zur Erstellung eines Notfallmediums.

### 1.1.2 Drive Crypt Plus Pack installieren

Um DCPD zu installieren starten Sie die Setup.exe und folgen den Anweisungen.

Nachdem Sie die Lizenzbestimmungen akzeptiert haben, können Sie den Ordner bestimmen, in den DCPD installiert werden soll. Nach der Installation werden sie aufgefordert ihren Computer neu zu starten. Nach dem notwendigen Neustart können Sie mit der Verschlüsselung Ihrer Festplatte/en fortfahren.

### 1.1.3 Drive Crypt Plus Pack löschen

Um DCPD von Ihrem Computer gehen sie über Start-> Systemsteuerung -> Software, dort wird DCPD als „Drive Crypt Plus Pack (Programmversion)“ angezeigt. Die automatische Deinstallation starten sie mit einem Klick auf „OK“.



## 2. DCPD benutzen

### 2.1 Erstellung eines Key Stores

Der erste Schritt, zur Benutzung von DCPD, ist die Erstellung eines Key Stores. Der Key Store kann als Schlüssel Datenbank oder als Schlüsselkasten angesehen werden. Es ist ein Lager für erstellte und importierte Schlüssel. Jeder Schlüssel, der erstellt oder importiert wird, wird automatisch im Key Store gespeichert. Es können mehrere Key Stores auf demselben Computer erstellt werden, jeder ist einzeln passwortgeschützt. Die Erstellung eines Key Store wird mit einem Assistenten automatisiert.

Um einen Key Store zu erstellen, gehen Sie wie folgt vor:

Nach dem Start von Drive Crypt Plus Pack erscheint das folgende Fenster:



Klicken Sie auf den „**Create**“ Button.

Das folgende Fenster wird geöffnet:

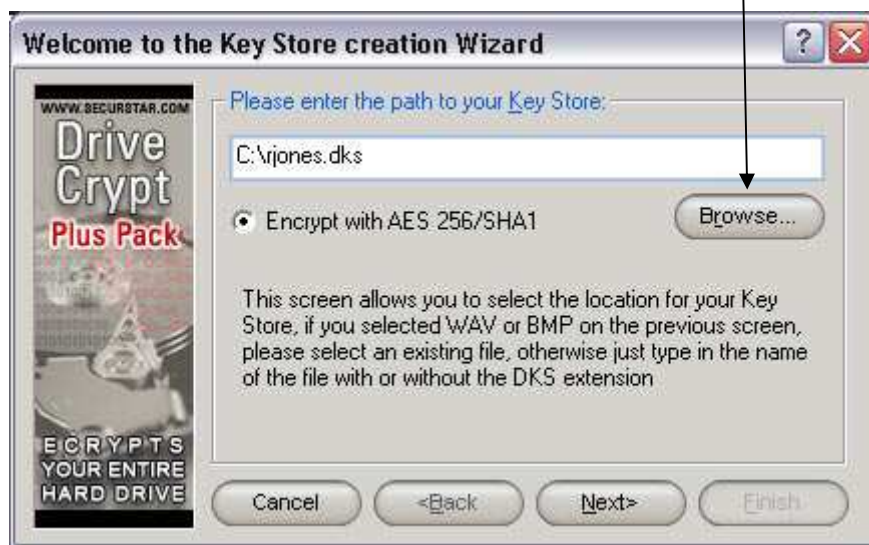


Hier kann ausgewählt werden wie und wie der Key Store gespeichert werden soll (als normale Datei, in einem .BMP Bild, in einer .WAV Musikdatei oder auf einem USB- Token)

Wenn Sie nicht sicher sind, belassen Sie die Einstellung so und klicken auf „Next“.

In dem nächsten Fenster können Sie den Pfad auswählen, indem der Key Store gespeichert werden soll. In dem Beispiel heißt der Key Store „rjones.dks“ und ist auf der Festplatte „C:“ gespeichert. Um den Namen zu ändern setzen Sie für „rjones“ einen beliebigen Namen ein (.dks **muss** am Ende stehen bleiben!)

Den Pfad können Sie ändern, indem Sie auf „**Browse...**“ klicken.



Klicken Sie auf „**Next**“ um zum letzten Fenster zu gelangen.

In dem letzten Fenster können Sie die Passwörter wählen, mit denen Sie auf Ihre Festplatte zugreifen können.

Sie können ein oder zwei verschiedene Passwörter benutzen.

Beachten Sie, dass die Passwörter *case sensitive* sind. Das heißt, dass zwischen Groß- und Klein- Schreibung unterschieden wird!

**Achtung:** Wenn Sie die Englisch- sprachige Version benutzen, beachten Sie bei Passwörtern mit Sonderzeichen (ü, ö, ä, !, “, \$, usw.), dass Diese bei der Anmeldung eine andere Tastenbelegung haben! Schalten Sie das Eingabegebietsschema, bei der Passwortwahl, auf das „US“ Format oder halten Sie immer einen Ausdruck des Amerikanischen Tastaturlayouts bereit!  
(Erläuterung und Druckvorlage am Ende der Dokumentation)



Geben Sie die Passwörter wie folgt ein:

Reihe 1: Passwort1

Reihe 2: Passwort2

Reihe 3: Passwort1

Reihe 4: Passwort2

Wenn Sie nur ein Passwort benutzen wollen, geben Sie Dieses nur in die Reihe 1 und 3 ein. (2 u. 4 bleiben leer)

Mit einem Klick auf „**Show**“ können Sie die Passwörter sichtbar machen.

Wenn die Passwörter übereinstimmen klicken Sie auf „**Finish**“, nun ist der Key Store erstellt.

### 3. Anmeldung

Um Drive Crypt Pack Plus zu benutzen und Festplatten zu verschlüsseln müssen Sie sich vorher mit Ihrem Key Store anmelden. Klicken Sie auf „**Browse...**“ um Ihren Key Store auszuwählen. (Den Pfad haben Sie in 2.1 ausgewählt.)



Danach geben Sie die Passwörter ein, die Sie in vorher gewählt haben und klicken auf „**Login**“. (Wenn Sie nur ein Passwort gewählt haben, lassen Sie bitte die zweite Reihe frei.)

## 4. Schlüssel

### 4.1 Schlüssel Überblick

Nachdem Sie sich das erste Mal angemeldet haben, müssen Sie einen neuen Schlüssel erstellen. Die Schlüssel werden für die Ver- und Entschlüsselung, der Festplatte, benutzt; alle Schlüssel werden in dem Key Store gespeichert.

Jeder Schlüssel wird zufällig von DCPD generiert, die Einzige, das benötigt wird ist eine Beschreibung des Schlüssels. Diese kann von Ihnen frei gewählt werden (z.B. „Festplatte C“ oder Hauptschlüssel).

Ein Schlüssel kann aktiv oder inaktiv sein, aber nur ein aktiver Schlüssel kann zur Verschlüsselung genutzt werden.

Hier können Schlüssel auch importiert, exportiert sowie gelöscht werden.

Um einen neuen Schlüssel zu erstellen gehen Sie wie folgt vor:

Klicken Sie links auf „**KEYS**“ und danach rechts auf „**New Key**“



Darauf werden Sie dieses Fenster sehen:



Um nun einen Schlüssel zu erstellen geben Sie bitte eine beliebige Beschreibung ein und klicken auf „**Generate**“

Der nun erstellte Schlüssel kann nun zur Verschlüsselung benutzt werden.

## 5. Laufwerke

### 5.1 Laufwerks Überblick

Laufwerke werden übersichtlich von DCPD angezeigt und können mit wenig Aufwand ver- sowie entschlüsselt werden. Um die Laufwerke zu sehen klicken Sie bitte auf den „**Drives**“ Button.



Bevor Sie Ihre Boot Partition verschlüsseln wollen müssen Sie vorher Bootauth installieren.



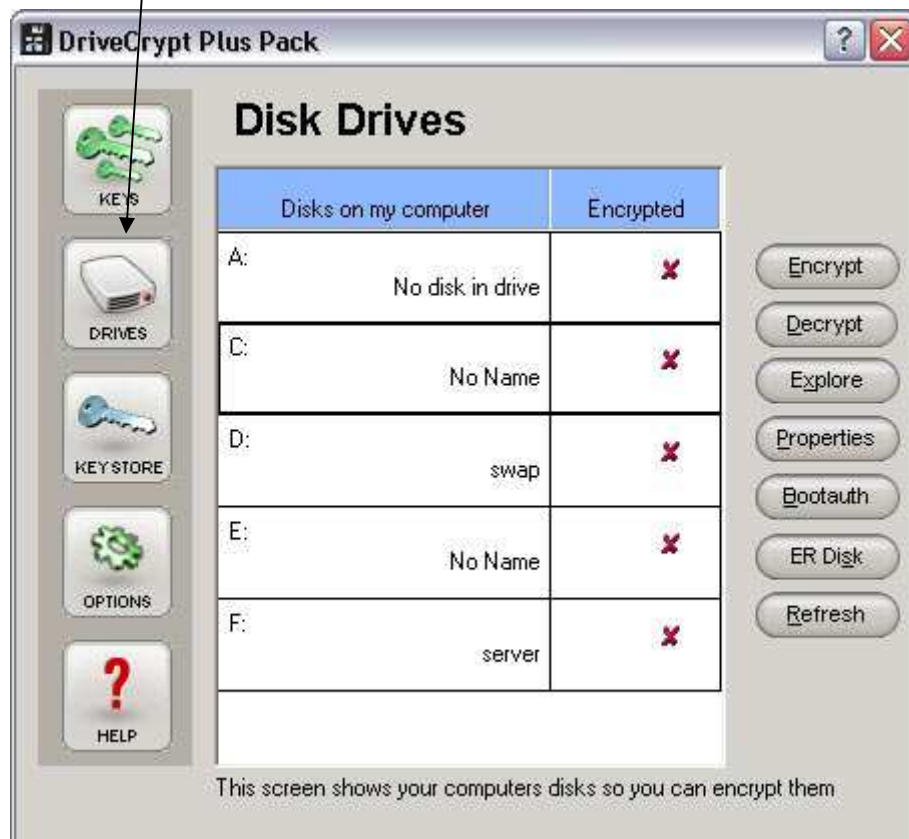
## 6. Bootauth

### 6.1 Bootauth Überblick

Bootauth ermöglicht eine Anmeldung vor dem booten, um Windows zu starten müssen Sie sich hier vorher anmelden, somit ist es ein Extraschutz für Ihren Computer. Bootauth wird auf der Standard Bootpartition( meist C:) installiert und beinhaltet eine grafische Anmeldeoberfläche.

### 6.2 Bootauth Installation

Um Bootauth zu installieren klicken Sie bitte auf den „Bootauth“ Button auf dem Laufwerksüberblick.



In dem folgendem Fenster klicken Sie bitte auf „**Next**“



Darauf erscheint dieses Fenster:



Wenn Sie einen USB- Token benutzen, können Sie hier wählen wie Sie ihr System in der Zukunft starten wollen (nur Passwort, nur Token oder mit einer Kombination aus Passwort und Token).

Wenn Sie keinen Token benutzen, klicken Sie bitte einfach auf „**Next**“.

Nun wird sich ein weiteres Fenster öffnen.



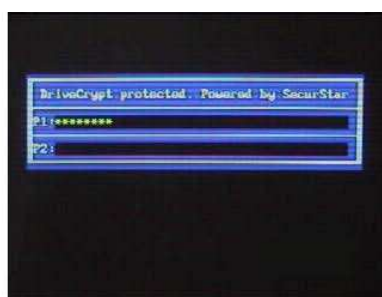
Hier können Sie auswählen wie Bootauth angezeigt werden soll, folgende Anzeigemethoden können gewählt werden:

- Vesa fancy; Hier wird ein grafisches Anmeldefenster angezeigt
- Dos simple; Hier wird ein Dos Anmeldefenster angezeigt (benutzen Sie diese Option wenn Sie eine nicht kompatible VESA Grafikkarte benutzen).
- Black HDD fail; Verwenden Sie diese, wenn Sie nicht wollen das Jemand erkennt, das Sie DCPD benutzen. Es wird eine authentische Fehlermeldung angezeigt.

Hier Screenshots der verschiedenen Methoden:



VESA fancy



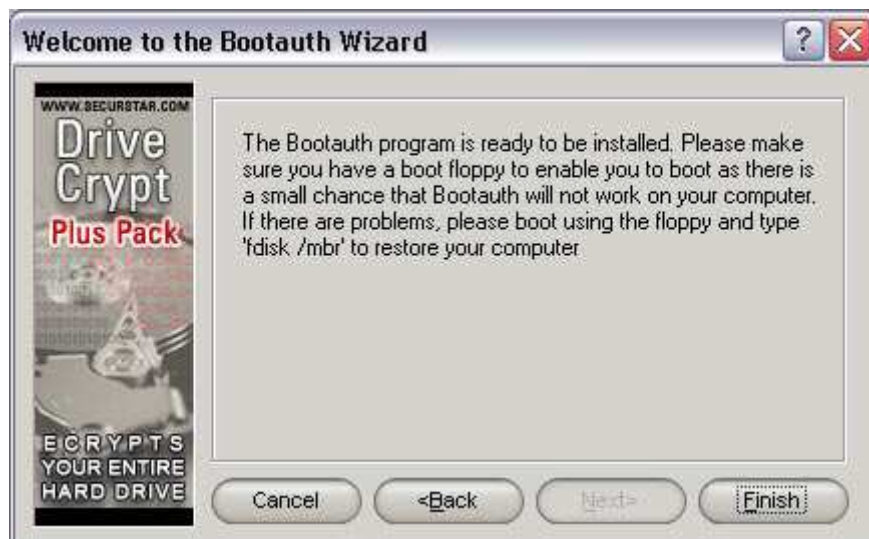
Dos Simple



Black HDD Fail

Bitte wählen Sie eine Methode und klicken Sie auf „**Next**“.

Das folgende Fenster wird nun angezeigt:



Um die Bootauth Installation abzuschließen klicken Sie bitte auf „Finish“.

Darauf wird folgende Meldung angezeigt:



„Ihr Computer wurde erfolgreich geändert. Zur Sicherheit starten Sie bitte den Computer neu um zu überprüfen ob das Bootauth Programm richtig funktioniert. Bei dem Start sollte dann das Passworteingabefeld erscheinen, indem Sie die, zuvor gewählten, Passwörter eingeben können müssen, um Windows starten zu können.

### **Problembehandlung:**

In seltenen Fällen kann es passieren, dass der Computer keine Vesa kompatible Grafikkarte enthält und sie den Computer nicht starten können, in dem Fall können booten Sie den Computer mit einer MS- Dos Startdiskette und führen den Befehl „FDISK/MBR“ aus (ohne „“). Alternativ können Sie auch das Rettungsmedium benutzen. Somit wird Bootauth deinstalliert. Bitte führen Sie die obige Bootauthinstallation erneut aus und wählen die „Dos simple“ Methode aus.

## 7. Anmelden in DCPD

### 7.1 Anmeldung

Um Drive Crypt Plus Pack zu benutzen und Laufwerke verschlüsseln und entschlüsseln zu können, müssen Sie sich vorher mit einem Key Store anzumelden - wie Sie es schon einmal unter 3. getan haben.

Klicken Sie bitte auf „**Browse...**“, um den Key Store auszuwählen.

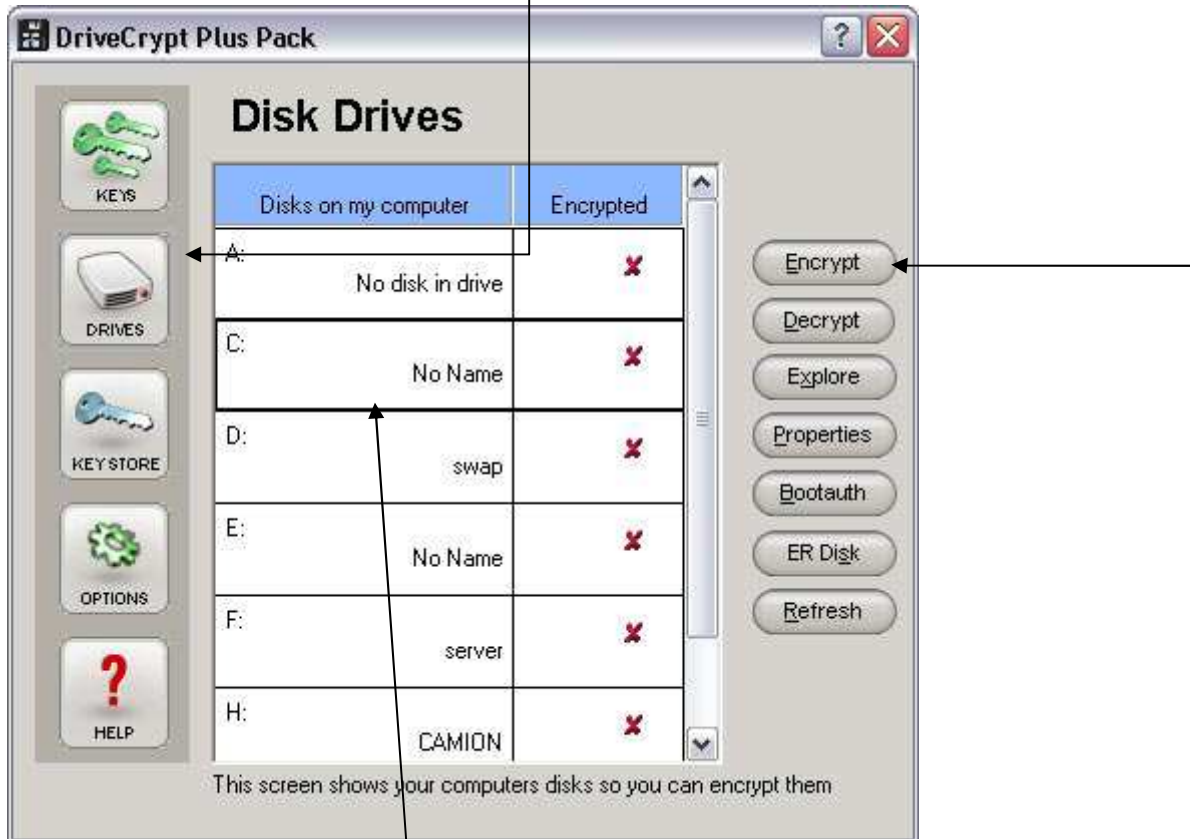


Nachdem Sie den Key Store ausgewählt haben, geben Sie bitte Ihr Passwort ein und klicken danach auf „**Login**“.

## 8. Verschlüsseln eines Laufwerks

### 8.1 Verschlüsseln eines Laufwerks

Um ein Laufwerk zu verschlüsseln klicken Sie bitte auf „**Drives**“ um so auf zu der Laufwerksübersicht zu gelangen.



Wählen Sie dann den Laufwerksbuchstaben, mit einem Klick, aus, den sie verschlüsseln wollen und klicken auf den „**Encrypt**“ Button.

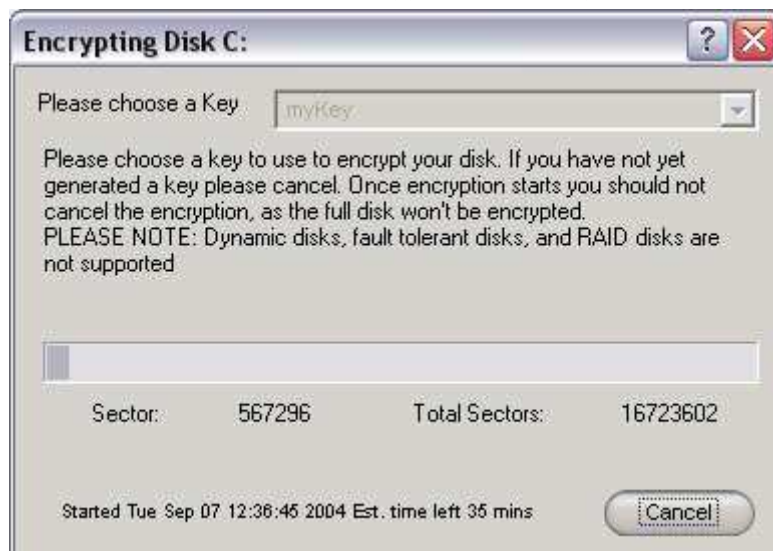
Folgendes Fenster wird sich öffnen:





Hier können Sie den Schlüssel auswählen, mit dem Sie das Laufwerk verschlüsseln wollen. Wenn Sie noch keinen Schlüssel erstellt haben, fahren Sie bitte zunächst mit dem Punkt 4. fort. Haben Sie ein Schlüssel ausgewählt klicken Sie auf **„Encrypt“**.

Nach dem Klick auf „Encrypt“ wird folgendes Fenster geöffnet.



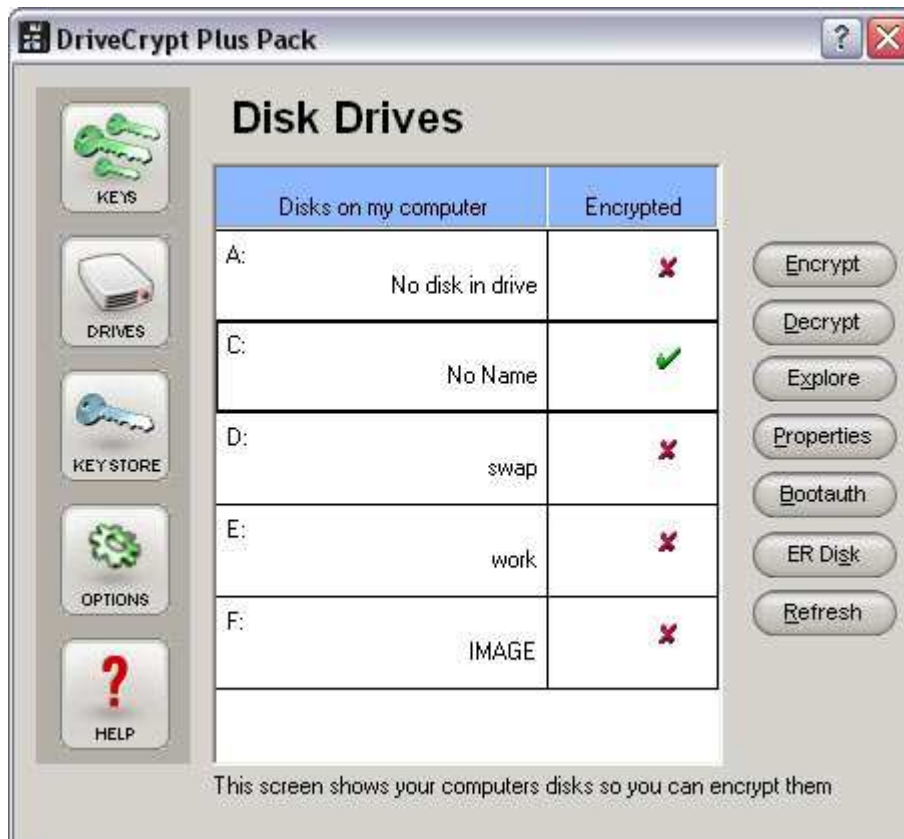
Nachdem der Verschlüsselungsvorgang beendet ist, wird bei Erfolg dieses Fenster erscheinen:



Nach einem Klick auf „OK“ ist das Laufwerk verschlüsselt und wird nun in der Laufwerksübersicht mit einem grünen Haken angezeigt.

## 9. Notfall- Reparatur Medium erstellen

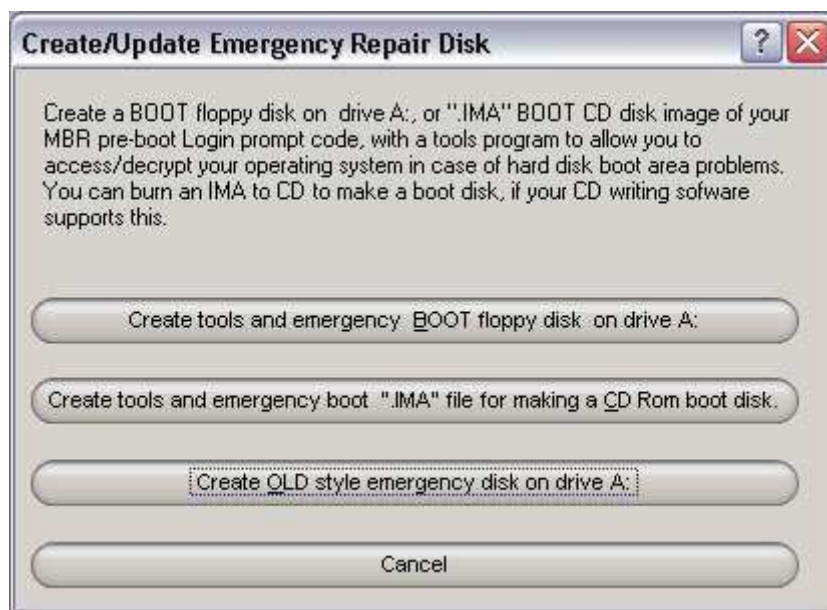
Nach der Installation von Bootauth und der Verschlüsselung eines Laufwerks ist es ratsam ein Medium, zur Wiederherstellung in einem Fehlerfall, zu erstellen. Bei einem Festplattenproblem können Sie ihren Computer mit diesem Medium starten.



Klicken Sie bitte in der Laufwerksübersicht den „ER Disk“ Button.

Dann werden Sie zu dem folgendem Fenster geleitet:





Hier haben Sie 3 Möglichkeiten zur Erstellung eines Rettungsmediums:

- **„Create tools and emergency BOOT floppy disk on drive A:“**  
Erlaubt das Starten des Computers, sowie die Ver- und Entschlüsselung von einer Diskette. (Empfohlen)
- **„Create tools and emergency boot „.IMA“ file for making a CD Rom boot disk“**  
Erstellt eine .IMA Datei, die benutzt werden kann um bootbare CD- Roms zu erstellen. Erlaubt das speichern von Wiederherstellung- Infos und Rettungs Programmen auf einer CD- Rom.

Die meisten Brennprogramme erlauben es bootbare CD- Roms zu erstellen. Die Bootinformationen werden in einer .IMA Datei gespeichert. So eine Datei erstellt DCPD bei dieser Methode.

Wenn Sie eine bootbare CD- Rom mit Ihrem Brennprogramm erstellen, stellen Sie sicher, dass Sie die .IMA Datei für die Bootinformationen, der CD- Rom, ausgewählt haben.

(Ob Ihr Brennprogramm das Erstellen von bootbaren CD- Roms unterstützt und wie Sie diese mit Ihrer Software erstellen können entnehmen Sie der Hilfedatei der Brennsoftware)

- **„Old Style emergency disk“**

Hier wird nur Bootauth auf eine Diskette kopiert. Hiermit können Sie das Laufwerk nur starten und nicht entschlüsseln.

Bitte wählen Sie eine der obigen Methoden aus, um ein Rettungsmedium zu erstellen.

**Achtung:** Die „Old Style emergency disk“ Methode benötigt für ihre Erstellung nur einige Sekunden und Sie werden im Explorer keinen Zugriff auf diese Diskette haben, trotzdem wird sie, wenn Sie den Computer bei einem beschädigtem MBR starten wollen, Sie zum Anmeldebildschirm bringen.

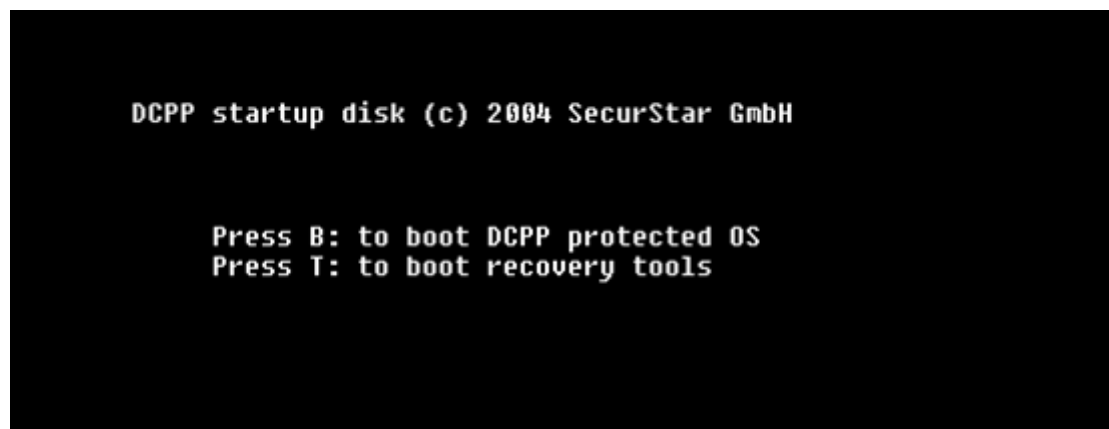
## 10. Notfall- Reparatur Medium einsetzen

### Benutzen des Notfallmediums

Wenn Ihr Betriebssystem nicht mehr startet, können Sie das erstellte Notfallmedium (Diskette oder CD- Rom) dazu benutzen um Ihr(e) Laufwerk(e) manuell zu entschlüsseln. Nachdem Sie das(die) Laufwerk(e) entschlüsselt haben, können Sie Fehler beheben oder das System neu installieren, ohne Daten zu verlieren.

Das Notfallmedium kann Ihnen auch helfen, werden der MBR von einem Programm (o.Ä.) gelöscht wurde und Sie somit nicht mehr zu dem Anmeldebildschirm gelangen.

Bitte starten Sie ihren Computer mit dem Notfallmedium (CD- Rom oder Diskette) in einem bootbaren Laufwerk.



Wenn Sie von einem Notfallmedium starten haben Sie folgende Optionen:

**<B>:** Startet das geschützte Betriebssystem.

Benutzen Sie diese Option wenn der MBR fehlerhaft ist oder ganz gelöscht wurde. Bei drücken der <B> Taste wird die Kopie von Bootauth, auf dem Medium, gestartet und Sie können Ihr Passwort eingeben. Bei erfolgreicher Anmeldung wird das Betriebssystem normal geladen. Wenn es geladen ist melden Sie sich bitte in DCPP an und führen die Bootauth- Installation erneut aus. (Punkt 6.2)

**<T>:** Startet Wiederherstellungsprogramme.

Diese Option ist für Probleme beim Start des Betriebssystems aufgrund eines allgemeinen Windowsfehlers.

Nach drücken der T- Taste haben sie die Möglichkeit das ganze Betriebssystem zu entschlüsseln und Zugang zu Ihren Daten zu bekommen. Einmal entschlüsselt, können Sie ihr Betriebssystem reparieren oder es neu installieren, ohne Daten zu verlieren.

**Achtung:** Das Wiederherstellungsprogramm kann nur dazu benutzt werden um die Bootpartition zu entschlüsseln (Die, auf der Ihr Betriebssystem liegt). Um andere Laufwerke zu entschlüsseln brauchen Sie direkten Windows Zugang zu DCPD.

Nachdem Sie <T> gedrückt haben, haben Sie mehrere Optionen:

```
DriveCrypt PlusPack version 3 Recovery tool

Press H: for HIDDEN OS DCPD disk recovery options
Press N: for NORMAL OS DCPD disk recovery options
Press M: to replace BOOTHAUTH with a standard Master Boot Record
Press Q: to quit
```

**H** – Erlaubt Ihnen ein verstecktes Betriebssystem wieder zu entschlüsseln.

Achtung: Wenn Sie ein verstecktes Betriebssystem wiederherstellen, wird das „falsche“ Betriebssystem gelöscht.

**N**– Erlaubt Ihnen die, mit DCPD verschlüsselte, Bootpartition zu entschlüsseln.

**Achtung:** Diese Option löscht ein eventuell vorhandenes Verstecktes Betriebssystem. Wenn Sie Ihr verstecktes Betriebssystem wiederherstellen wollen, nutzen Sie bitte Option **H**.

**M** – Löscht Bootauth von Ihrem Computer.

**Warnung:** Nutzen Sie diese Option nur, wenn Ihre Bootpartition nicht verschlüsselt oder Sie genau wissen was Sie tun. Wenn Sie Bootauth löschen, ohne es gesichert haben können Sie ihr Betriebssystem nicht mehr starten!

**Achtung!**

**Um ein Laufwerk mit dem Wiederherstellungsprogramm zu entschlüsseln, benötigen Sie trotzdem das Passwort, mit dem Sie es verschlüsselt haben!**

## 11. Verstecktes/ unsichtbares Betriebssystem

Betriebssystem wird im folgendem mit **OS** (Operating System) abgekürzt.

### Überblick

Drive Crypt Plus Pack ist geeignet um ganze Betriebssysteme in dem freien Speicherplatz eines anderen Betriebssystems zu verstecken.

Sie können zwei Passwörter für das mit DCPD verschlüsselte Laufwerk festlegen: Ein Passwort ist für das sichtbare Betriebssystem und ein Anderes für das Unsichtbare. Das erste Passwort verschafft Ihnen Zugriff auf das vorkonfigurierte OS, während Sie mit dem Anderen auf Ihr normales Betriebssystem, mit dem Sie arbeiten, zugreifen können.

Diese Funktion ist sehr hilfreich, wenn Sie fürchten, dass Sie jemand zwingen könnte das DCPD Passwort herauszugeben; in diesem Fall geben Sie das erste Passwort heraus und der „Angreifer“ wird nach dem starten, des Systems, nur die Informationen finden die Sie vorbereitet haben. Der „Angreifer“ wird keine geheimen oder persönlichen Daten finden, das versteckte OS wird ebenso nicht gefunden werden können. Wenn Sie aber ihr zweites, persönliches Passwort, eingeben, werden Sie Zugriff zu Ihrem System bekommen und auf Ihre geheimen Daten zugreifen können.

Ein verstecktes Betriebssystem ist für Niemanden sichtbar, ohne das richtige Passwort wird keiner bestimmen können ob dieses existiert.

### **Bevor Sie ein verstecktes Betriebssystem erstellen:**

Das versteckte OS ist ein Klon des ersten falschen Betriebssystems.

Sie können kein anderes oder neues OS installieren, das versteckte OS kann nur ein Klon des Ersten sein.

Sie können ein neues Betriebssystem über das Geklonte installieren, dies wird aber nicht empfohlen.

DCPD unterstützt nur Windows NT, 2000, XP und Vista

Als Größe der Bootpartition empfehlen wir 8- 9 GB.

**Lesen Sie den Punkt „Wo ist das unsichtbare Betriebssystem gespeichert“, in der programmeigenen Hilfedatei um zu lernen wie Sie die Bootpartition vorbereiten müssen und wie Sie den größtmöglichen freien Speicherplatz zu bekommen.**

## Erstellen des sichtbaren und des versteckten Betriebssystems:

Erstellen des, von außen sichtbaren, Betriebssystems:

1. Formatieren Ihre Festplatte/Bootpartition und installieren Sie Windows NT, 2000, XP oder Vista darauf.
2. Stellen Sie sicher, dass Sie die Bootpartition in FAT32 formatiert haben (Sie sollte mindestens 5GB groß sein, wir empfehlen aber mindestens eine Größe von 8GB.)

**Achtung:** Das sichtbare Betriebssystem **muss** in FAT32 formatiert sein, das versteckte OS kann aber in FAT32 oder NTFS formatiert sein.

3. Bereiten Sie das sichtbare OS so vor, wie es bei Eingabe des „falschen“ Passworts erscheinen soll.
4. Stellen Sie sicher, dass Sie mindestens die doppelte Größe, des verwendeten Speichers, auf der Bootpartition frei haben. (Wenn das Betriebssystem, mit den vorbereiteten Daten, 3GB Speicherplatz belegen benötigen Sie **mindestens** weitere 3GB freien Speicherplatz auf derselben Partition.)

## Erstellen des versteckten Betriebssystems

1. Installieren Sie DCPD und erstellen Sie 2 Key Stores mit jeweils einem Schlüssel(Lesen Sie dazu Punkt 2,3 und 4):

Der erste, „falsche“, Key Store wird benutzt um das „falsche“ sichtbare OS zu öffnen, der Zweite wird benutzt um das versteckte Betriebssystem zu verschlüsseln.

**Achtung:** Beide Key Stores müssen unterschiedliche Passwörter haben!

2. Melden Sie sich mit dem ersten, „falschem“, Key Store an und verschlüsseln Sie das Laufwerk(Dies ist nicht zwingend, wird aber empfohlen.). Starten Sie den Computer danach neu.
3. Starten Sie den Computer mit dem „falschen“ Passwort.  
Melden Sie sich in DCPD mit dem „falschen“ Key Store an und gehen auf die Laufwerksübersicht(**Drives**).



Wählen Sie den Laufwerksbuchstaben Ihrer Bootpartition aus(normal C) und klicken auf „**Hidden OS**“.

**Achtung:** Sie werden den Button „Hidden OS“ nur sehen, wenn die Bootpartition in FAT32 formatiert wurde.

Das folgende Fenster wird geöffnet:

The screenshot shows the 'DriveCrypt Plus Pack Hidden System Disk Creation Utility' window. It has a blue title bar with a logo on the left and a close button on the right. The window is divided into several sections:

- Technical information:** Contains fields for 'System' (set to 'C'), 'PhysDevice' (set to '\\Device\\Harddisk\\Volume1'), 'Total free space:', 'Total used:', 'Endblock size:', 'Endblock sect:', 'Int13h unit: 0', 'Startsect: 63', and 'Numsect: 10972332'.
- Creation progress and temporary disk information:** Contains 'Temporary source disk:' and 'Temporary dest disk:' fields, a progress bar, and the 'SecurStar' logo.
- Keystore file location and passwords for hidden disk access via Bootauth:** Contains a 'Path:' field with a 'Browse' button, 'Pass1:' and 'Pass2:' fields, and a note: 'The keystore and passwords MUST be different to the one you logged into DCPD with!'.
- Hidden disk label:** A text field containing 'HiddenOS'.
- Hidden disk type:** A dropdown menu set to 'FAT32'.
- Guard space before OS start:** A text field set to '20' followed by 'Megabytes'.

At the bottom center is a large button labeled 'Create Hidden OS'.

Klicken Sie auf Browse und wählen den zweiten, geheimen, Key Store aus (Mit diesem wird Ihr verstecktes OS verschlüsselt.).

In die Felder **Pass1** und **Pass2** müssen Sie die Passwörter eingeben, die Sie für den zweiten Key Store gewählt haben.

Optional können Sie die Laufwerksbeschreibung für das versteckte OS und die Art der Formatierung ändern (FAT32 oder NTFS).

In der rechten Ecke können Sie bestimmen wie viel Speicher zwischen den Beiden Betriebssystemen frei bleiben soll.

**Achtung:** Wir raten mindestens 20-100MB freien Speicherplatz zwischen den Betriebssystemen zu lassen.

Klicken Sie nun auf „**Create Hidden OS**“ um den Klon- Prozess zu starten. DCPD erstellt nun ein unsichtbares Laufwerk mit dem versteckten OS darauf. Nachdem der Prozess beendet ist, starten Sie Ihren Computer neu.

Jedesmal wenn Sie nun den Computer starten, können Sie entweder das „falsche“ Passwort in den DCPD Anmeldebildschirm eingeben(dann startet das vorbereitete OS) oder das Passwort für das versteckte (normale) Betriebssystem eingeben.

**Warnung: Wenn Sie das „falsche“ Betriebssystem verschlüsselt haben(Punkt 2 unter „Erstellen des versteckten Betriebssystems“.) ist das versteckte OS nicht verschlüsselt! Sie müssen dieses später ebenfalls verschlüsseln!**

**Test:**

Starten Sie das „falsche“ Betriebssystem um zu sehen ob alles ordnungsgemäß startet. **Warnung: Arbeiten Sie nicht mit dem „falschen“ OS und kopieren Sie keine Daten darauf!**

Starten Sie den Computer neu.

Starten Sie das versteckte OS um zu sehen ob alles ordnungsgemäß startet.

**Verschlüsseln des versteckten Betriebssystems:**

Nachdem das versteckte OS ordnungsgemäß gestartet ist, müssen Sie dieses verschlüsseln. Öffnen Sie dazu DCPD und melden Sie sich mit dem „geheimen“ Key Store an. Wählen Sie danach die Laufwerke die Sie verschlüsseln wollen. (Lesen Sie dazu Punkt 8)

Nach der Verschlüsselung starten Sie erneut um zu sehen ob alles ordnungsgemäß läuft. Bei Erfolg können Sie mit dem versteckten OS wie gewohnt arbeiten.

**Warnung:** Wir weisen hiermit darauf hin, dass sie das sichtbare Betriebssystem niemals unnötig starten sollten. Sie sollten auf keinen Fall damit arbeiten. Alle Daten, die auf dem „falschen“ OS kopiert oder verschoben werden könnten versteckte Daten auf dem versteckten Laufwerk überschreiben. Das „falsche“ Betriebssystem ist dazu da um das versteckte OS zu verbergen und ist nur für den Fall, das sie gezwungen sind das Passwort heraus zu geben.

**Achtung:** DCPD erlaubt es, ein verstecktes Laufwerk für ein verstecktes OS zu erstellen. Wenn Sie andere Laufwerk ebenso verschlüsseln und verstecken wollen, empfehlen wir eine Kombination aus DCPD und Drive Crypt. Drive Crypt bietet diese Funktion!

**Ratschlag:** Es ist immer ratsam Sicherheitskopien Ihrer Daten zu machen, unabhängig von Verschlüsselung oder nicht. Diese können Geld und Kopfschmerzen im Fall von Festplattenfehlern, Windowsfehlern usw. verhindern.

## **Eingabegebietsschema und amerikanische Tastaturbelegung zu Punk 2 .1**

Eingabegebietsschema auf amerikanisch umstellen:

„Start“ -> „Systemsteuerung“ -> „Regions- und Sprachoptionen“

„Registerkarte „Sprache“

„Textdienste und –eingabesprachen“ -> „Details“

„Standard- Eingabegebietsschema„-> „Englisch(USA) – US“

„OK“

## Amerikanische Tastaturbelegung:

USA

